UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,904	10/20/2004	Roger A Payne	36-1864	5056

23117 7590 08/17/2007

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
08/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/511,904	PAYNE ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on October 20, 2004. Claims 1-17 were originally received for consideration. A preliminary amendment for the claims was received on October 20, 2004.

2. Clams 1-17 are currently being considered.

Information Disclosure Statement

3. An initialed and dated copy of the Applicant's IDS form 1449, received on May 11, 2005, is attached to this Office action.

Specification

4. The specification does not contain any headings as delineated in 37 CFR 1.77(b). The guidelines suggested by the MPEP are given below.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.

(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

5. Claim 1 is objected to because of the following informalities: In the third line of the claim, it is stated "to transmit signals to at least one ***other*** link locking mechanism." However, there is no mention of a first linked locking mechanism in the claim, so there can be no ***other*** link locking mechanism. Furthermore, in lines 4-5 of the claim, it is stated "whereby access controlled by said at least one other locking mechanism is specifically permitted." This refers back to the other link locking mechanism. However, there is no first link locking mechanism. It is interpreted that the "other" is not meant to be in the claim language, and that it is "at least one linked locking mechanism." Appropriate correction is required.

6. Claims 4-5, and 9 are objected to because of the following informalities: Each of the aforementioned claims, in their 2nd lines, states "in which ***the or at one*** of said

locking mechanisms." It is believed that the phrase above is supposed to be "in which the at least one of said locking mechanisms." Appropriate correction is required.

7. Claim 1 is objected to because of the following informalities: In the fifth line of the claim, the word "validly" is in all capital letters, which it should not be. Appropriate correction is required.

8. Claims 10-11 are objected to because of the following informalities: Both claims contain the phrase "the controlling computer," which is has no antecedent basis in the claim or claim 1 in which they both depend. It is apparent that the controlling computer of the claims are referring to the computer system of claim 1, however, the claims still do not have an antecedent basis for a "controlling computer" and therefore, should be changed to resolve the problem. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-5, 8-13, 15, and 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Kucharczyk et al. (U.S. Patent 6,570,488).

Regarding claim 1, Kucharczyk discloses:

An information security system comprising a computer system (column 3, lines 55-59: *computer servers*) responsive to the presence of an identifiable entity (column 4, lines 43-44: "*person making such access*") to permit access to the computer system (column 7, lines 23-29: *wherein an access code can only be received if identifying information is provided to the computer system*) and to transmit signals to at least one other linked locking mechanism (column 4, lines 53-58: *transmitter emits signal to access code entry unit*) to cause said locking mechanism to release (column 4, lines 57-58: *the locking mechanism is unlocked*) whereby access controlled by said at least one other locking mechanism is specifically permitted while said computer system is validly accessible (column 8, lines 19-32), *wherein when multiple access codes are needed to keep a device unlocked, the computer server has to be able to process requests for new access codes and issue new access codes for a given time frame*.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the locking mechanism includes a time means which in the absence of period release signals inhibits access after a predetermined time period expires (column 8, lines 19-32),

wherein multiple access codes are needed to keep the device unlocked for a given time frame, and if the time period expires, new codes will not be provided, inhibiting access to the device.

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which a plurality of locking mechanisms each controlling access to a respective entity are provided (Figure 3, items 32, 34, 36, column 6, lines 58-64), *wherein there are multiple locking devices in the system.*

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the or at one of said locking mechanism is associated with a respective lockable physical object (column 4, lines 52-53, column 12, lines 9-13), *wherein lockable physical object is a storage device, a door, a gate, and other security systems.*

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the or at one of said locking mechanisms is associated with a respective electronic or electrical

equipment whereby use of such electronic or electrical equipment is only permitted while an authorized user is present (column 5, lines 41-45), *wherein locking mechanism can include electronics such as cameras, which can only be accessed and thereby used, if an authorized user unlocks the locking mechanism.*

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 including shared facilities responsive to signals from a plurality of computers each responsive to a respective identifiable entity to permit usage of such shared facilities (Figure 3, column 3, line 65 – column 4, line 3), *wherein a plurality of access devices can gain access to a storage device, but only if they have an access code.*

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the or each locking mechanism is also responsive to signals from an alternative source to permit access without requiring access to a computer of the system (column 4, lines 51-58), *wherein the signal can be sent from an infrared transmitter instead of directly received from the server (Figure 3, item 30).*

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claim in claim 1 in which the locking mechanism is in wired communication with the controlling computer (column 6, lines 34-43), *wherein the locking mechanism can be connected to the server (controlling computer) via a dedicated network connection.*

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the or each controlling computer includes radio transmission arrangements (column 6, lines 43-45: "RF interfaces") whereby following authorised access the computer causes periodic transmission of coded release signals whereby correspondingly coded radio transmission receivers linked provide release instructions to respective locking mechanisms (column 8, lines 19-32), *wherein multiple access codes are needed to keep the device unlocked for a given time frame, and if the time period expires, new codes will be periodically supplied via different interfaces, including RF interfaces which can be either public or private.*

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 11 in which the transmission of release signals from a computer may be inhibited if the computer enters a temporary inhibition of access (column 8, lines 49-57), *wherein if the access codes are not used in a certain period of time, the computer system (server) is configured to automatically cancel the code, thus inhibiting access to the secured device.*

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 12 in which the transmission of release signals is inhibited in the absence of entry of data thereto for a predetermined period (column 8, lines 49-57), *wherein if the access codes are not used in a certain period of time, the computer system (server) is configured to automatically cancel the code, thus inhibiting access to the secured device.*

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which at least one of said locking mechanisms requires the presence of more than one authorised individual (column 4, lines 28-53), *wherein the server (one authorized individual) is needed to provide the access codes and a second individual is needed to either manually enter the access code or use a transmitter to open the storage device (locking mechanism).*

Regarding claim 17, Kucharczyk discloses:

An office environment comprising at least one computer (column 3, lines 55-59: *computer servers*) and at least one linked lockable device (column 4, lines 52-53, column 12, lines 9-13: *wherein the lockable device could be a door, gate, or storage device*), the computer being responsive to an authorised identifiable entity to effect unlocking of the lockable device to permit access to the device while said identifiable entity is present (column 7, lines 25-40), *wherein an authorized user gets an access code which is used by the authorized user to unlock a lockable device.*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 6-7, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. (U.S. Patent 6,570,488) in view of Hasebe (U.S. Patent 5,987,609).

Claim 6 is rejected as applied above in rejecting claim 1. Kucharczyk does not explicitly disclose telecommunication control means arranged to control usage of communication lines whereby telephony or facsimile may be inhibited in the absence of an appropriately authorised user. Hasebe discloses a system for remotely locking a wireless information

device by sending a message to the phone, which is checked against a stored password, and if the phone is not authenticated, it is locked (Hasebe: column 6, lines 33-59). Kucharczyk and Hasebe are analogous arts because both teach methods of remotely locking devices using a cellular network. Kucharczyk invites the combination with Hasebe by stating (the locking device may be used with doors, gates, and other security systems (Kucharczyk: column 12, lines 6-11) not limiting the use of the security method to any environment. Furthermore, Kucharczyk teaches a system where the access codes (equivalent to the message containing the password of Hasebe) are sent over a cellular network (Kucharczyk: Figure 3, item 40). It would have been obvious to incorporate the method of Hasebe of locking phones with the system of Kucharczyk, so that "in the case where the information device should be lost or stolen, the leakage of data to others can be prevented" (Hasebe: see Abstract).

Claim 7 is rejected as applied above in rejecting claim 6. Kucharczyk does not explicitly disclose telecommunication control means arranged to control usage of communication lines whereby telephony or facsimile is limited in usage to prevent certain categories of call or communication. Hasebe discloses a system for remotely locking a wireless information device by sending a message to the phone, which is checked against a stored password, and if the phone is not authenticated, it is locked (Hasebe: column 6, lines 33-59). Kucharczyk and Hasebe are analogous arts because both teach methods of remotely locking devices using a cellular network. Kucharczyk invites the combination with Hasebe by stating (the locking device may be used with doors, gates,

and other security systems (Kucharczyk: column 12, lines 6-11) not limiting the use of the security method to any environment. Furthermore, Kucharczyk teaches a system where the access codes (equivalent to the message containing the password of Hasebe) are sent over a cellular network (Kucharczyk: Figure 3, item 40). Hasebe discloses that the user can set different security levels on the phone, so that the level of communication when the communication is inhibited varies amongst, screen lock, or data erase (column 6, lines 44-55). It would have been obvious to incorporate the method of Hasebe of locking phones with the system of Kucharczyk, so that "in the case where the information device should be lost or stolen, the leakage of data to others can be prevented" (Hasebe: see Abstract).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Kucharczyk discloses:

An information security system as claimed in claim 1 in which the computer system is linked to a telecommunications system (Figure 3, item 42, column 6, lines 45-50: *wherein the server is connected through a PSTN*) and transmits information defining the identity of the authorised user present (column 7, lines 23-35), *wherein the access codes are provided for authorized users and are used to unlock devices.*

Kucharczyk does not explicitly disclose whereby associated telecommunication devices receive facilities and communications appropriate to the respective identified authorized user. Hasebe discloses a system for remotely locking a wireless information device by

sending a message to the phone, which is checked against a stored password, and if the phone is not authenticated, it is locked (Hasebe: column 6, lines 33-59). Kucharczyk and Hasebe are analogous arts because both teach methods of remotely locking devices using a cellular network. Kucharczyk invites the combination with Hasebe by stating (the locking device may be used with doors, gates, and other security systems (Kucharczyk: column 12, lines 6-11) not limiting the use of the security method to any environment. Furthermore, Kucharczyk teaches a system where the access codes (equivalent to the message containing the password of Hasebe) are sent over a cellular network (Kucharczyk: Figure 3, item 40). It would have been obvious to incorporate the method of Hasebe of locking phones with the system of Kucharczyk, so that "in the case where the information device should be lost or stolen, the leakage of data to others can be prevented" (Hasebe: see Abstract).

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. (U.S. Patent 6,570,488) in view of Dowling et al. (U.S. Patent 6,548,967).

Kucharczyk does not explicitly disclose an environmental control arrangement whereby at least one of lighting, heating and ventilation are controlled in dependence upon the presence or absence of one or more users. Dowling discloses a system using smart lighting devices, which can receive, and process signals over a network, which can activate or deactivate a lighting device based on a password (Dowling: column 21, lines

21-34). Dowling and Kucharczyk are analogous arts because both provide passwords (access codes) over a network to allow an authorized user use of a device. Kucharczyk has the foundation necessary for the system of Dowling to function in that it provides PSTN, and network connections to different secured areas, which are the connections used by Dowling to provide the smart lighting devices with signals. Furthermore, the passwords (Dowling: column 30-33), which are used with the control unit of Dowling, are analogous to the access codes provided by the computer server of Kucharczyk. Kucharczyk invites the combination with Hasebe by stating (the locking device may be used with apartment buildings, doors, gates, and other security systems (Kucharczyk: column 12, lines 6-11) not limiting the use of the security method to any environment. Therefore, it would have been obvious to one of ordinary skill in the art to use the lighting system of Dowling in the system of Kucharczyk "to moderate access control to various sites of a building" (Dowling: column 11, lines 44-46) and "to maintain privacy of data available from the lighting network 208, and to prevent unauthorized tampering with devices attached to the lighting network 208" (Dowling: column 21, lines 31-35).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kaveh Abrishamkar 7/14/07
Kaveh Abrishamkar
AU 2131

KA
KA
08/14/2007